ABSTRACT

A method and apparatus are described for a one-way broadcast distribution of keys for decrypting encrypted broadcast content. According to one embodiment of the present invention, a method and apparatus are described for generating a list of update keys on a content provider system based on a table of secret keys associated with a plurality of content receivers. The list of update keys is generated in a manner to allow valid receivers to recover a valid content key while invalid receivers recover an invalid content key. The list of update keys are used to generate a multiple nested list of decryption patterns that is broadcast to all receivers. The receivers then recover an appropriate set of update keys for each receiver from the multiple nested list of decryption patterns so that the final key recovered in the set of update keys is a content key.